Notice of Allowability	Application No.	Applicant(s)	
	09/955,924	HUITEMA ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Interview on 1/13/2006*.

2. ☒ The allowed claim(s) is/are *2-8 and 10-25*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *1/13/2006* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

Primary Examiner
AU 2131
1/26/06

DETAILED ACTION

Claims 2 – 25 have been presented for examination. Claims 9 has been cancelled and claims 2, 5, 8 and 10 have been amended in an amendment filed 11/10/2005.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/10/2005 has been entered.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Carole A. Boelitz (Reg. No. 48,958) on 11/10/2005.

This application has been amended as follows:

IN THE CLAIMS

Cancel claim 1 and 9 without prejudice.

Replace claim 2, 8, 13 and 18 as follows.

Claim 2: A method of inviting and joining a peer to a secure peer-to-peer group comprising the steps of:

obtaining a public key (P_{U1}) of a peer;

forming, by a first member of the group, a group membership certificate containing the peer's public key (P_{U1}) and signed with a group private key (K_G) of a group public/private key pair, the group membership certificate having a structure of $((P_{U1})K_G)$;

sending the group membership certificate from the first member to the peer to invite the peer to join the group, the group membership certificate allowing the peer to join the group through a second member other than the first member;

receiving, at a second member of the group different from the first member, a connect message from the peer containing the group membership certificate signed by a private key of the peer, the connect message requesting connection to the secure peer-to-peer group;

the second member, authenticating the group membership certificate before allowing the peer to connect to the secure peer-to-peer group; and

if the group membership certificate is authenticated, sending an accept message to the peer including a group shared key.

Claim 8: In a secure peer-to-peer group having a predefined public/private key pair (P_G/K_G), a method of inviting a peer to join the group, comprising the steps of:

obtaining a public key (P_{U1}) of a peer by a first member of the peer-to-peer group;

forming by the first member a first group membership-certificate containing the peer's public key (P_{U1}) and a second group membership certificate signed with the group private key (K_G), ~~the first group membership certificate being~~ and signed with a private key of the first member (K_{U2}), the second group membership certificate having a structure of $((P_{U1})K_G)K_{U2}$);

sending the first and second group membership certificates from the first member to the peer to invite the peer to join the group; ~~and~~

receiving, at a second member different from the first member, a connect message from the peer containing the first group membership certificate; and

if the first group membership certificate is authenticated, sending an accept message to the peer including a group shared key.

Claim 13: A method of securely joining a peer-to-peer group by a peer having a public key (P_{U1}) and a private key (K_{U1}), comprising the steps of:

receiving a group invitation from a first member containing an invitation certificate ~~having~~ a group ID ~~provided therein~~, the invitation certificate including the public key of the peer (P_{U1}) signed by a private key (K_G) of the peer-to-peer group;

resolving the group ID to find a third member of the group different from the first member;

sending a connect message to the third member containing the invitation certificate signed with the private key (K_{U1}) of the peer and having a structure of $((P_{U1})K_G)K_{U1}$;

receiving an accept message from the third member containing a group membership certificate signed by a private key (P_3) of the third member; and

receiving a group shared key to enable decryption of group traffic.

Claim 18: A method of securely admitting a peer to a peer-to-peer group, comprising the steps of:

receiving at a first member of the peer-to-peer group, a connect message from the peer containing an invitation certificate generated by a second member of the peer-to-peer group and signed by a private key (K_{U1}) of the peer, the first member being different from the second member, the invitation certificate containing a public key of the peer (P_{U1}) signed by a group private key (K_G), the invitation certificate signed by the private key (K_{U1}) of the peer having a structure of $((P_{U1})K_G)K_{U1}$;

authenticating the invitation certificate signed by the peer's private key (K_{U1}); and

when the step of authenticating is successful,

sending an accept message to the peer from the first member, and

sending a group shared key to the peer.

Allowable Subject Matter

1. Claims 2 – 8 and 10 – 25 are allowed.
2. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claim 2 and subsequent dependent claims.

The prior arts Turnbull, alone or in combination with Aoki, fail to teach or suggest process steps and/or elements that constitutes peer-to-peer name resolution protocol (PNRP) group security of inviting and joining a peer to a secure peer-to-peer group, as recited in the pending claims. Therefore, the CPA does not teach or suggest the claimed invention in the following way: obtaining a public key (P_{U1}) of a peer; forming, by a first member of the group, a group membership certificate containing the peer's public key (P_{U1}) and signed with a group private key (K_G) of a group public/private key pair, the group membership certificate having a structure of ((P_{U1})K_G); sending the group membership certificate from the first member to the peer to invite the peer to join

the group, the group membership certificate allowing the peer to join the group through a second member other than the first member; receiving, at a second member of the group different from the first member, a connect message from the peer containing the group membership certificate signed by a private key of the peer, the connect message requesting connection to the secure peer-to-peer group; the second member, authenticating the group membership certificate before allowing the peer to connect to the secure peer-to-peer group: and if the group membership certificate is authenticated, sending an accept message to the peer including a group shared key.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

Primary Examiner
AU 2131
1/26/06